DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AIR INTELLIGENCE AGENCY CHECKLIST 31-2

29 September 2000

Security

INFORMATION SECURITY, PERSONNEL SECURITY, INDUSTRIAL SECURITY, AND PHYSICAL SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil.

OPR: HQ AIA/SOX (MSgt Guy Woodbury) Certified by: HQ AIA/SOX (CMSgt Thomas Hughes)
Pages: 32
Distribution: F

This checklist is a guide for effective management. It is not a directive and is not an authority to establish or implement procedures. It may contain items that are not governed by directives; however, these items are based on proven management principles. *NOTE:* Using the name of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

1. How to Use This Checklist. Chiefs of Security Forces or unit security managers may use the applicable portions of this checklist to monitor and evaluate their security programs. Other staff agencies and, or personnel may use this checklist to evaluate their own internal security programs.

2. Baseline Checklist. This publication establishes a baseline checklist. The checklist will also be used by the agency Inspector General (IG) during applicable assessments. Use the attached checklist as a guide only. Add or modify each area as needed, to ensure an effective and thorough review of the unit security program. See Attachment 2.

3. Where to Find Guidelines. Each question in this checklist is referenced to its governing directives. See Attachment 1.

JIMMY R. JONES
Chief of Security

Attachment 1

GLOSSARY OF REFERENCES

References

E.O. 12958, *Classified National Security Information*

DoD 5200.1-R, *DoD Information Security Program*

DoD 5220.22-M, *National Industrial Security Program Operating Manual*

AFPD 31-4, *Information Security*

AFI 31-401, *Information Security Program Management*

AFPD 31-5, *Personnel Security Program Policy*

AFI 31-501, *Personnel Security Program Management*

AFH 31-502, *Personnel Security Program*

AFPD 31-6, *Industrial Security*

AFI 31-601, *Industrial Security Management Program*

AFI 31-101, *AF Installation Security Program*

DoD 5105.21-M-1, *SCI Administrative Security Manual*

Joint DoDIIS/Cryptologic SCI Information Systems Security Standard

AFMAN 14-304, *The Security, Use, and Dissemination of SCI*

DCID 1/7, *Security Controls on the Dissemination of Intelligence Information*

DCID 6/4, *Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to SCI*

DCID 1/19, *Security Policy for SCI and Security Policy Manual*

DCID 1/21, *Physical Security Standards for SCIFs*

DCID 5/6, *Intelligence Disclosure Policy*

AFI 16-701, *Special Access Programs*

AFI 10-1102, *Safeguarding Single Integrated Operational Plans (SIOP)*

DCID 6/2, *Technical Surveillance Countermeasures*

DCID 6/3, *Protecting SCI within Information Systems*

USSAN 1-69, (U) *US Implementation of NATO Procedures* (C)

AFI 31-101/AIA Sup 1, *Installation Security Program*

Attachment 2

INFORMATION SECURITY, PERSONNEL SECURITY, INDUSTRIAL SECURITY, AND PHYSICAL SECURITY

A2.1. Security Functional Areas for Inspection:

Table A2.1. Checklist for Information Security.

SECTION 1: INFORMATION SECURITYMISSION STATEMENT: Promote proper and effective classification, protection and downgrading of official information requiring protection in the interest of the national security.			
1.1. CRITICAL ITEMS. Security Education and Training:	**YES**	**NO**	**N/A**
1.1.1. Is the unit fulfilling the requirements of the AIA Security, Training, Education, and Motivation (STEM) program? (AFI 31-401, AIA Sup 1, paragraph 10.6)			
1.1.2. Are program reviews (self-inspections) conducted, documented, and follow-up actions taken? (DoD 5200.l-R, paragraph 1-202d and AFI 31-401, paragraph 1.4.3)			
1.1.3. Does the unit's Security, Education, and Training Program meet established requirements? (E.O. 12958 and AFMAN 14-304, paragraph 12.3.4)			
1.1.4. Is training provided to Original Classification Authorities (OCA), if applicable? (DoD 5200.1-R, paragraph 2-202)			
1.1.5. Are classified documents marked in accordance with the following? (E.O. 12958, DoD 5105.21-M-1, and ROXADs 99-10 and 99-15)			
1.1.5.1. Classification markings at the top and bottom of the document?			
1.1.5.2. Appropriate control markings?			
1.1.5.3. Paras and sub-paras markings?			
1.1.5.4. Classified by or Derived from statements?			
1.1.5.5. Declassify on statements? (date, event, or exemption)			
1.2. NONCRITICAL ITEMS. Security Official Responsibilities:	**YES**	**NO**	**N/A**
1.2.1. Are primary and alternate SCI security officials appointed in writing? (DoD 5105.21-M-1, chapter 1, section F, paragraph 4)			
1.2.1.1. Special Security Officer (SSO)			
1.2.1.2. Special Security Representative (SSR)			
1.2.1.3. TK Control Officer (TCO)			
1.2.1.4. Gamma Control Officer (GCO)			
1.2.1.5. BYE Control Officer (BCO)			
1.2.2. Are the grade requirements of a military commissioned officer, warrant officer, or civilian (GS-9 or above) met for the position of SSO? (DoD 5105.2-M-1, chapter 1, section F, paragraph 5a)			

1.2.3. Are up-to-date copies of the appropriate DoD Directives and Manuals, including DoD 5105.21-M-1 and AFMAN 14-304 readily available? (DoD 5105.21-M-1, chapter 1, section F, paragraph 5a(2))			
1.2.4. Is there program oversight to ensure proper protection, use, and dissemination of SCI documents and materials? (DoD 5105.21-M-1, chapter 1, section F, paragraph 4b)			
1.2.5. Is there a memorandum of agreement (MOA) with other organizations, as necessary, on SCI areas of responsibility, training, operational needs, support and services? (DoD 5105.21-M-1, chapter 1, section F, paragraph 4f)			
1.2.6. Are Standard Operating Procedures (SOPs) developed for unique processes in the Security Office? (DoD 5105.21-M-1, chapter 1, section K)			
1.2.7. Is initial security training provided by the security manager or supervisor? (AFI 31-401, paragraph 8.3.1 and DoD 5200.1-R, paragraph 9-200a)			
1.2.8. Has the security manager received prescribed training for his or her duties? (AFI 31-401, paragraph 8.7.2.2)			
1.2.9. Has the Information Security Program Manager (ISPM) established a system to identify Air Force and localized training requirements? (AFI 31-401, paragraph 8.8)			
1.2.10. Are the security requirements for storage, handling, transmission, and destruction of Top Secret material being met? (AFI 31-401, paragraph 5.10)			
1.2.11. Are the appropriate cover sheets being used to shield classified information? (AFI 31-401, paragraph 5.11.1 & 5.11.2 and DoD 5105.21-M-1, chapter 3, section K)			
1.2.12. Are secure facsimile controls established? (DoD 5105.21-M-1, chapter 3, section J)			
1.2.13. Do individual header or cover sheets precede the transmission of all SCI facsimiles? Are individual headers or cover sheets signed by the receiver and returned as a receipt of accountable SCI? (DoD 5105.21 -M-1, chapter 3, section J)			
1.2.14. Are “accountable SCI documents” brought under control and assigned Document Accountability Numbers, if applicable? (DoD 5105.21-M-1, chapter 3, section N, paragraph 1)			
1.2.15. Are receipts used for the transfer of documents outside of an organization and, or SCIF? (DoD 5105.21-M-1, chapter 3, section M, paragraph 4b)			
1.2.16. Are burn bags properly marked? (DoD 5105.21-M-1, chapter 3, section U, paragraph 6)			
1.2.17. Are the security requirements for the storage, handling, transmission, and destruction of NATO material as outlined in (U) USSAN 1-69 (C), United States Implementation of NATO Security Procedures being met? (DoD 5200.1-R and DoD 5100.55)			
1.2.18. Are couriers trained and briefed prior to conducting courier duties? (DoD 5105.21-M-1, chapter 3, section S, paragraph 3)			

1.2.19. Do briefcases used for the transportation of classified material have a luggage tag affixed annotating that it is U.S. Government Property and shall be returned unopened? (DoD 5105.21-M-1, chapter 3, section T, paragraph 2)			
1.2.20. Is each container (safe, file cabinet, map cabinet, etc.) containing SCI material identified for emergency destruction and, or removal? (DoD 5105.21-M-1, chapter 5, section H, paragraph 4)			
1.2.21. Is classified information (not designated as being of historical value) not required for effective and efficient operation of the organization being properly secured, handled, and destroyed beyond reconstitution in a timely manner? (DoD 5200.1-R, paragraph 6-700a, and DoD 5105.21-M-1, chapter 3, section U, paragraph 2)			
1.2.22. Are appropriate Standard Form (SF) 700 series being used? (AFI 31-401, paragraph 5.23.2, 4.6, and 5.11)			
1.2.23. Is there a current threat assessment on file? (DoD 5105.21-M-1, chapter 1, section E, paragraph 2)			
1.2.24. Are files or folders marked with the highest classification of the material contained within? (DoD 5105.21-M-1, chapter 3, section I, paragraph 8)			
1.2.25. Are working papers marked appropriately? (DoD 5105.21-M-1, chapter 3, section H)			
1.2.26. Are all removable Automated Information System (AIS) media items properly labeled? (DCID 3/14, Annex B)			
1.2.27. Are collateral intelligence incidents reported and processed as required? (AFPD 14-3, ROXAD 05-99)			
1.2.28. Are SCI security incidents reported within 72 hours to HQ AIA/SOC? (DoD 5105.21-M-1, chapter 4, section D, paragraph 1 and ROXAD 5-99)			
1.2.29. Are SCI security incident interim reports provided every 30 days to HQ AIA/SOC? (DoD 5105.21-M-1, Chapter 4, Section D, paragraph 1)			
1.2.30. Are SCI incidents classified according to content? (DoD 5105.21-M-1, chapter 4, section D, paragraph 1)			
1.2.31. Are security incident case files retained as required? (DoD 5105.21-M-1, chapter 4, section H)			
1.2.32. Are incidents (both SCI and collateral intelligence) involving Information Systems classified accordingly and reported to the appropriate organizations? (DoD 5105.21-M-1, chapter 4, section C, paragraph 6 and ROXAD 5-99)			
1.3. North Atlantic Treaty Organization (NATO):			
1.3.1. Are NATO briefings recorded on AF Form 2583, **Request for Personnel Security Action**? (AFI 31-401, AFI 31-501, and AFH 31-502, paragraph 2.11)			
1.3.2. Is NATO restricted information limited to persons who officially need it to perform their assigned duties? ((U) USSAN 1-69 (C), paragraph 29)			

1.3.3. Are NATO debriefings recorded on AF Form 2587, Security Termination Statement? (AFI 31-401, paragraph 1-4.1)			
1.3.4. Is AF Form 1565, **Entry Receipt and Destruction Certificate**, used to document destruction of COSMIC Top Secret document page changes? (AFI 31-401, paragraph 9.1.3)			
1.3.5. Are annual rebriefings given to individuals cleared for ATOMAL access? ((U)USSAN 1-69 (C), Attach 1, paragraph 53 (C))			
1.3.6. Are individuals debriefed whenever an individual goes on a PCS assignment, separates, terminates federal service, or no longer requires access? ((U) USSAN 1-69 (C), Attach 1, paragraph 33)			
1.3.7. Are classification markings, downgrading instructions, etc., applied on NATO material as required? ((U) USSAN 1-69 (C), Atch 1, paragraph 27 (C))			
1.3.8. Do subregistry or control point officers assign reference numbers for COSMIC Top Secret, NATO Secret, and accountable ATOMAL documents that activities they service prepare? (USSAN 1-69(U), Atch 1, paragraph 60 (C))			
1.3.9. Are AF Form 310, **Document Receipt and Destruction Certificate**, or DD Form 1565, used to document destruction of NATO Secret material? (AFI 31-401 and (U) USSAN 1-69 (C))			
1.3.10. Are 100 percent inventories of all COSMIC Top Secret being conducted annually or when there is a change in NATO control officer? ((U) USSAN 1-69 (C), Atch 1, paragraph 81 (C))			
1.3.11. Do sub-registries maintain reports of investigation pertaining to compromise of NATO material? (AFI 31-401, paragraph 9.1.3)			
1.3.12. Are combinations to security containers holding NATO material changed at least every six months? ((U) USSAN 1-69 (C), paragraph 60a)			
1.4. Top Secret Control:			
1.4.1. Is a Top Secret Control Account established for the origination, storage, receipt, and dispatch of Top Secret material? (AFI 31-401, paragraph 5.10.1.1)			
1.4.2. Is a Top Secret Control Officer, with at least one alternate, designated? (AFI 31-401, paragraph 5.10.1.1)			
1.4.3. Is the AF Form 144 being used and is it attached to the applicable Top Secret material? (AFI 31-401, paragraph 5.10.1.2.1)			
1.4.4. Is the AF Form 143 used to account for each document, piece of material, or piece of equipment? (AFI 31-401, paragraph 5.10.1.1)			
1.4.5. How is AIS or microfiche media accounted for? (AFI 31-401, paragraph 5.10.1.1)			
1.4.6. Is an annual inventory conducted for all Top Secret material in the account? (AFI31-401, paragraph 5.10.1.3.1)			
1.4.7. Is an inventory conducted whenever there is a change in TSCOs? (AFI 32-401, paragraph 5.10.1.3.1)			

1.4.8. Are procedures established to process Top Secret facsimiles? (AFI 31-401, paragraph 5.10.1.5)			
1.4.9. Are two people with Top Secret access involved in the destruction of Top Secret material? (AFI 31-401, paragraph 5.29.2.1.1)			
1.5. SIOP-ESI:			
1.5.1. Are personnel requiring SIOP access briefed to the proper category and is the briefing recorded on AF Form 2583? (AFI 10-1102, paragraph 6.1)			
1.5.2. Is AF Form 2587 utilized to record debriefings from SIOP? (AFI 10-1102, paragraph 6.3)			
1.5.3. Who is your SIOP-ESI access granting authority? (AIA Sup to AFI 10-1102, paragraph 5.2.2.1)			
1.5.4. Do you annually report, to HQ AIA/SOP, all persons approved for SIOP-ESI access? (AIA Sup to AFI 10-1102, paragraph 5.2.2.1)			
1.6. CNWDI			
1.6.1. Is clearance and need-to-know established prior to release of CNWDI information? (DoDD 5210.2, paragraph 2.a(5))			
1.6.2. Is the requirement for "full justification" of need-to-know adequate? (DoDD 5210.2 paragraph F.1.(b)(3))			

Table A2.2. Checklist for Personnel Security.

SECTION 2: PERSONNEL SECURITYMISSION STATEMENT: Foster mission accomplishment by ensuring military, civilian, reserves, and contractor personnel worldwide attain and maintain personnel security standards established by the Director of Central Intelligence Directives with reasonable assurance against compromise of sensitive compartmented information (SCI.)			
2.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
2.1.1. Security Information File (SIF):			
2.1.1.1. Does the unit have a copy of AFI 31-501, *Personnel Security Program Management*, dated 1 Aug 00 and AFMAN 14-304? (HQ USAF or SFI letter, Revisions to AFI 31-501, *Personnel Security Program Management*)			
2.1.1.2. Does the commander establish a SIF when an individual's activity, conduct, or behavior is inconsistent with the security criteria specified in DoD 5200.2-R, paragraph 2-200, Appendix I and DCID 6/4? (AFI 31-501, paragraph 8.2.1.2. and AFMAN 14-304, paragraph 2.5.2.6)			
2.1.1.3. Does the commander establish SIFs on individuals within their jurisdiction, including: (AFI 31-501, paragraph 8.2.1.1.)			
2.1.1.3.1. Tenants or geographically separated units; and			
2.1.1.3.2. TDY personnel when unfavorable information is reported or developed, which directly impacts on an individual's security clearance eligibility or SCI access?			

2.1.1.4. Does the commander determine whether or not to establish a SIF on a case-by-case basis within 20 working days after receipt of derogatory information? (AFI 31-501, paragraph 8.2.1.3, AFMAN 14-304, paragraph 2.5.2.5)			
2.1.1.5. Is the CAF notified within 10 days after deciding to establish a SIF (AFMAN 14-304, paragraph 2.5.2.5 and AFI 31-501, para 2.2.3.)			
2.1.1.6. Prior to establishing a SIF, does the commander consider the following: (AFI 31-501, paragraph 8.2.1.3)			
2.1.1.6.1. the seriousness of the incident,			
2.1.1.6.2. the individual's motivation,			
2.1.1.6.3. whether the incident was out of character for the individual, and;			
2.1.1.6.4. whether the undesirable conduct or behavior is likely to continue?			
2.1.1.7. Does the commander consult with the servicing Special Security Officer prior to establishing a SIF? (AFI 31-501, paragraph 8.2.1.3)			
2.1.1.8. Does the commander notify the person in writing when a SIF has been established? (AFMAN 14-304, paragraph 2.5.2.6)			
2.1.1.9. Does the commander determine whether or not to initiate interim suspension action for SCI access or to suspend an individual's access to classified information or unescorted entry to restricted areas upon establishment of a SIF? (AFI 31-501, paragraph 8.2.1.4, AFMAN 14-304, paragraph 2.5.3)			
2.1.1.10. Is the decision to suspend an individual's access to SCI or classified information based upon a thorough review of the facts and an assessment of the risk to national security? (AFI 31-501, paragraph 8.2.1.4)			
2.1.1.11. If the decision is to suspend an individual's SCI access, does the commander notify the individual, in writing, of the suspension of SCI access and the reason for such action consistent with the interests of national security? (DOD 5105.21-M-1, paragraph I.2(a) and AFI 31-501, para 8.2.1.5.)			
2.1.1.12. Are suspensions of SCI access reported to AIA/SOPS within 24 hours? (AFMAN 14-304, paragraph 2.5.3 and AFI 31-501, para 8.2.1.4.)			
2.1.1.13. Unless authorized by the AIA unit commander, are individual's who have had their SCI access suspended, or have received a final denial or revocation of security clearance, denied access to AIA SCIFs or restricted areas, even while under escort? (AFI 31-101, AIA Sup 1, paragraph 5.3.9.6)			
2.1.1.14. Does the commander provide a recommendation whether to grant, deny, or revoke the individual's security clearance eligibility and, or SCI access eligibility in the final SIF? (AFI 31-501, paragraph 8.2.1.7.)			
2.1.1.15. Do the documented facts of the SIF fully support the commander's decision to grant, deny, or revoke the individual's security clearance eligibility and, or SCI access eligibility? (AFI 31-501, paragraph 8.2.1.6.)			
2.1.1.16. When special circumstances exist (i.e., individual was falsely accused or holds a special expertise that is essential for mission accomplishment), does the Commander request immediate closure of the SIF via priority message to 497 IG/INSA through the MAJCOM SSO? (AFI 31-501, paragraph 8.2.1.8.)			

2.1.1.17. Does the Chief of the Servicing Security Activity or Special Security Office provide guidance to commanders on SIF establishment? (AFI 31-501, paragraph 8.2.2.1.)			
2.1.1.18. Does the Chief of the Servicing Security Activity or Special Security Office establish, maintain, monitor, and forward SIFs to SSO AIA/SOPS? (AFI 31-501, paragraph 8.2.2.2.)			
2.1.1.19. Does the Chief of the Servicing Security Activity or Special Security Office forward the SIF to the gaining servicing activity or SSO when a change of assignment occurs? (AFI 31-501, paragraph 8.2.2.6.)			
2.1.1.20. Does the Chief of the Servicing Security Activity or Special Security Office process SIFs expeditiously? (AFI 31-501, paragraph 8.2.2.3)			
2.1.1.21. Does the Chief of the Servicing Security Activity or Special Security Office forward initial SIFs to SSO AIA/SOPS with an information copy to the 497 IG/INSO and each intermediate headquarters (i.e., 26 IOG, 67 IOG, 692 IOG, 694 IG, and the 67 IOW, AND 70 IW)? (AFI 31-501, paragraph 8.2.2.3)			
2.1.1.22. Does the Chief of the Servicing Security Activity or Special Security Office notify SSO AIA/SOPS, with an information copy to the 497 IG/INSO and each intermediate headquarters (i.e., 26 IOG, 67 IOG, 692 IOG, 694 IG, 67 IOW, and 70 IW), when an individual's access has been reinstated by the unit commander? (AFI 31-501, paragraph 8.2.2.3)			
2.1.1.23. Do all initial SIFs contain at least the following information: (AFI 31-501, paragraph 8.2.2.3. and AFMAN 14-304, Figure 2.5)			
2.1.1.23.1. Full name?			
2.1.1.23.2. Grade or Rank?			
2.1.1.23.3. Social Security Number?			
2.1.1.23.4. Base assigned?			
2.1.1.23.5. Date SIF was established?			
2.1.1.23.6. SSBI date?			
2.1.1.23.7. Accesses?			
2.1.1.23.8. Reason for SIF establishment?			
2.1.1.23.9. Investigations conducted, pending?			
2.1.1.23.10. Date access suspended or rationale for nonsuspension of access?			
2.1.1.23.11. POC?			
2.1.1.24. When SIFs are forward via facsimile transmission, is the CAF notified telephonically before transmission? (AFMAN 14-304, Figure 2.5)			
2.1.1.25. Does the Chief of the Servicing Security Activity or Special Security Office follow the provisions of AFMAN 14-304, Chapter 2 when unfavorable information results in discharge, or court-martial, of an individual who is or has been SCI indoctrinated within the past three years? (AFI 31-501, paragraph 8.2.2.3.1.)			

2.1.1.26. Does the Chief of the Servicing Security Activity and Special Security Office notify the 497 IG/INSO when an adverse discharge is overturned and the individual is returned to active duty? (AFI 31-501, paragraph 8.2.2.3.2)			
2.1.1.27. Does the Chief of the Servicing Security Activity or Special Security Office request evaluations and relevant documentation from the following activities when the issue involved indicates coordination is appropriate: (AFI 31-501, paragraph 8.2.2.5)			
2.1.1.27.1. Director of Personnel: reviews the individual's UIF, performance report summaries, and personnel actions required as a result of the individual's behavior.			
2.1.1.27.2. Security Forces: reviews for criminal activities or other pertinent data regarding the subject's police record, involvement in previous compromises or security incidents.			
2.1.1.27.3. Judge Advocate: determines if any court proceedings or nonjudicial punishment is legally supportable by nature of individual's actions.			
2.1.1.27.4. Surgeon General: conducts an evaluation of any physical, mental, or emotional state which may affect the subject's ability to protect classified information.			
2.1.1.27.5. Mental Health Clinic: reviews for any involvement, previous or present, with alcohol or dangerous drugs which may indicate a security weakness.			
2.1.1.28. Does the Chief of the Servicing Security Activity or Special Security Office ensure all supporting documentation is included prior to submitting the SIF for closure? Note: The following are types of required documentation relevant to the issue: (AFI 31-501, paragraph 8.2.2.9.)			
2.1.1.28.1. PSI conducted by DIS, OPM, or similar agencies.			
2.1.1.28.2. AFOSI reports of investigation, civil police, or child advocacy reports.			
2.1.1.28.3. Security police incident or complaint reports and special security office reports.			
2.1.1.28.4. A summary of facts to substantiate and unfavorable information not covered by one of the investigative sources above. (**NOTE:** A complete reference to the source of the information must be included.)			
2.1.1.28.5. A summary of Unfavorable Information File (UIF) entries.			
2.1.1.28.6. Medical or mental health evaluations which indicate significant impairment of the individual's judgment or reliability. Does the evaluation:			
2.1.1.28.6.1. Contain a diagnosis and its effect on the individual's judgment and reliability?			
2.1.1.28.6.2. Contain a prognosis?			
2.1.1.28.6.3. Any additional restrictions or instructions on the use of the information by appropriate medical authority?			
2.1.1.28.7. Summary of actions by Social Actions, to include the following:			

2.1.1.28.7.1. Date enrolled in the program?			
2.1.1.28.7.2. Reason for enrollment?			
2.1.1.28.7.3. Categorization of the individual's situation?			
2.1.1.28.7.4. Diagnosis?			
2.1.1.28.7.5. Social Actions authorities recommendations regarding clearance eligibility?			
2.1.1.28.8. The date of successful completion of a rehabilitation program, progress in a rehabilitation program or the date termed a rehabilitative failure was declared.			
2.1.1.28.9. A summary or actual report of administrative or disciplinary actions to include:			
2.1.1.28.9.1. Letters of counseling.			
2.1.1.28.9.2. Letters of reprimand.			
2.1.1.28.9.3. UCMJ Article 15 actions.			
2.1.1.28.9.4. Court-martial orders.			
2.1.1.28.9.5. Bankruptcy petitions.			
2.1.1.28.9.6. Discharge orders.			
2.1.1.28.9.7. Copies of letters of indebtedness.			
2.1.1.28.10. Orders or written notification advising the status and location of individuals placed:			
2.1.1.28.10.1. In retraining.			
2.1.1.28.10.2. On appellate leave.			
2.1.1.28.10.3. In rehabilitation status.			
2.1.1.28.10.4. In confinement status.			
2.1.1.28.11. Correspondence or forms relating to the withdrawal of access, including special access programs, unescorted entry, or decertification from PRP.			
2.1.1.29. Are completed SIFs forwarded through AIA/SOPS to the CAF within 120 days? (AFMAN 14-304, paragraph 2.5.2.8 and AFI 31-501, para 8.2.2.7.)			
2.1.1.30. Does the Chief of the Servicing Security Activity or Special Security Office maintain a record copy of the SIF until 6-months after the unit loses accountability of the individual? (AFI 31-501, paragraph 8.2.2.11.)			
2.1.1.31. Has the unit Security Manager implemented the personnel security program within the organization? (AFI 31-501, paragraph 8.2.3.)			
2.1.1.32. Has the unit Security Manager provided support to the supporting security forces activity or special security office? (AFI 31-501, paragraph 8.2.3.)			
2.1.2. "For Cause" Program:			
2.1.2.1. Does the commander request permission to proceed in court-martials, administrative discharges, and civilian removal actions who have had SCI access within the past 3 years? (AFMAN 14-304, paragraph 2.5.5)			

2.1.2.2. Does the unit commander consult the following people while preparing the request to discharge message: (JGUBY 07-99)			
2.1.2.2.1. Staff judge advocate.			
2.1.2.2.2. Program security manager.			
2.1.2.2.3 Senior intelligence officer.			
2.1.2.3. Are "For Cause" requests transmitted through the Defense Special Security Communications System (DSSCS)? (AFMAN 14-304, paragraph 2.5.5)			
2.1.2.4. Are requests for authority to proceed forwarded through SSO channels, to SSO AIA/SOPS, with information copies to SSO USAF or INSDM, and each intermediate headquarters (67 IW, 26 IG, 67 IG, 692 IG, 694 IG) as appropriate? (AFMAN 14-304, paragraph 2.5.5)			
2.1.2.5. Are classified requests for authority to proceed: (JGUBY 07-99)			
2.1.2.5.1. properly portion marked, to include subject lines;			
2.1.2.5.2. classified according to content;			
2.1.2.5.3. and marked in accordance with EO 12958 by having the classification block identified (Derived From:..., Declassify On:...)?			
2.1.2.6. Do requests for authority to proceed contain the following: (JGUBY 07-99)			
2.1.2.6.1. Personal data:			
2.1.2.6.1.1. Name?			
2.1.2.6.1.2. Grade?			
2.1.2.6.1.3. SSN?			
2.1.2.6.1.4. Date of birth?			
2.1.2.6.1.5. Place of birth?			
2.1.2.6.1.6. Marital status?			
2.1.2.6.1.7. Number of dependents?			
2.1.2.6.1.8. Total active federal military service date (TAFMSD)?			
2.1.2.6.1.9. Date of separation?			
2.1.2.6.1.10. Organizational commander's name?			
2.1.2.6.1.11. Unit of assignment?			
2.1.2.6.1.12. Duty title?			
2.1.2.6.1.13. AFSC?			
2.1.2.6.1.14. Whether or not the person was a system administrator or had root access to an automated information system (AIS)?			
2.1.2.6.1.15. A description of the AIS to which the subject had root access to and, or was a system administrator, the highest level of classification processed on the AIS?			
2.1.2.6.1.16. A commander's assessment of the potential damage to local or national interests if the subject were to infiltrate, corrupt, sabotage, or otherwise damage the AIS subject has had root access to or was system administrator for?			

2.1.2.6.1.17. The likelihood the subject of a DFC would infiltrate, corrupt, sabotage, or otherwise damage the AIS subject had root access to or was system administrator for?			
2.1.2.6.1.18. Actions taken to protect affected AIS?			
2.1.2.6.2. Access Data:			
2.1.2.6.2.1. Date SCI access was first granted?			
2.1.2.6.2.2. Access level or categories?			
2.1.2.6.2.3. Units involved?			
2.1.2.6.2.4. Frequency of handling?			
2.1.2.6.2.5. Date access terminated?			
2.1.2.6.2.6. Debriefing date?			
2.1.2.6.3. Access history (including specific compartments, sub-compartments, and "B" accesses for the past three years). (**NOTE:** Access history should contain at least: depth of access, systems and dates, projects and dates, and previous accesses.)			
2.1.2.6.4. Incident and background. (**NOTE:** This section should include details of the incident, whether there will be any local publicity, whether or not a SIF has been established, any and all previous offenses or incidents, and any administrative and, or disciplinary actions.)			
2.1.2.6.5. Proposed disciplinary or administrative action. (**NOTE:** Included in this sections are the maximum penalty that could be levied by court-martial. If being discharged, this section should contain the worst possible characterization that could be administered and the commander's characterization recommendation. It should cite specific articles of the UCMJ and, in the case of discharge actions, cite the specific paragraph member is being discharged under.)			
2.1.2.6.6. Commander or local SIO evaluation of information. (NOTE: This section *must* include the impact to national security (minimal or serious). It will also contain information pertaining to the perishability of the information, factors for special consideration, and any other information bearing on the proposed action.)			
2.1.2.6.7. Commander's assessment of the member. (**NOTE:** The commander's estimate of the person's ability to comprehend and remember details, including their overall knowledge, attitude, and inquisitiveness, and assesses their attitude towards the Air Force and toward being discharged.) Does the commander include any other significant facts known about the individual including:			
2.1.2.6.7.1. Any attempts to expand access to classified information by repeatedly volunteering for special assignments which would require additional access, or inquiring about classified information which the individual has no need-to-know?			
2.1.2.6.7.2. Unauthorized removal of classified material from the workplace?			

2.1.2.6.7.3. Any documents charged or signed out to the individual which could not be accounted for during annual inventory or inspections?			
2.1.2.6.7.4. Repeated or unusual overtime?			
2.1.2.6.7.5. Falsifying destruction records?			
2.1.2.6.7.6. Sudden unexplained affluence?			
2.1.2.6.7.7. A pattern of recurring travel, either in the US or abroad, without apparent recreation or business purposes?			
2.1.2.6.7.8. Falsification of locations visited on either leave statements or travel vouchers?			
2.1.2.6.7.9. Travel to communist countries, or country hostile to the US?			
2.1.2.6.7.10. Repeated association with non-US citizens, regardless of nationality?			
2.1.2.6.7.11. Any known financial problems?			
2.1.2.6.7.12. Any known medical problems?			
2.1.2.6.7.13. Based upon items 1 through 12 above, has the commander determined the following?			
2.1.2.6.7.13.1. Is the person subject to blackmail, defection, or exploitation?			
2.1.2.6.7.13.2. Does the person harbor any bitterness or resentment as a result of the adverse action?			
2.1.2.6.7.13.3. Will the person continue to protect special access information?			
2.1.2.6.8. Judge advocate certification:			
2.1.2.7. Are follow-up reports submitted every 90-days until closure has been received from SSO AIA? (JGUBY 07-99)			
2.1.2.8. Do final reports include type, date, and place of discharge? (JGUBY 07-99 and AFI 31-501, para 8.9.12.)			
2.1.3. SCI Eligibility:			
2.1.3.1. Are requests for SSBIs on all individuals requiring SCI access submitted? (DCID 6/4, paragraph 7a)			
2.1.3.2. Does the unit use the Automated Security Clearance and Approval System (ASCAS) roster to determine eligibility for access to classified material? (AFI 31-501, paragraphs 7.4)			
2.1.3.3. Does the unit have a compelling need program? (DoD 5105.21-M-1, chapter 2, paragraph H.1)			
2.1.3.4. Are all requirements, to include a favorable screening interview, met for a compelling need prior to submitting request? (DoD 5105.21-M-1, chapter 2, paragraph h.1 (a-d) and Appendix E-Annex 2)			
2.1.3.5. Have unit commanders implemented programs to continuously evaluate unit personnel for trustworthiness and reliability? (AFI 31-501, paragraph 9.1.1.1)			

2.1.3.6. Are all military personnel who have been determined eligible for SCI access been 'S' coded in the unit-manning document (UMD)? (AFI 31-501, paragraph 7.2)			
2.1.3.7. Is AF Form 2583, **Request for Personnel Security Action**, used to conduct local files checks? (AFI 31-501, paragraph A2.6)			
2.1.3.8. Does the authorized requester ensure Periodic Reinvestigations (PR) are not submitted on personnel who are within 12 months of an established retirement or separation date? (DoD 5105.21-M-1, Chapter 2, Paragraph F.L.C.)			
2.1.3.9. Are required Single Agency Checks (SAC), on spouses, family members, and cohabitants, submitted for personnel who require SCI access? (AFI 31-501, paragraph 3.4.3)			
2.1.3.10. Does the authorized requester promptly notify the Air Force Liaison at Defense Security Service (DSS) to cancel pending investigations which are no longer required due to separation, job change, etc.? (DoD 5200.2-R, Appendix C, paragraph A.5)			
2.1.4. Access Management (Indoctrinations):			
2.1.4.1. Does the unit have a professional and effective SCI-indoctrination process? (DoD 5105.21-M-1, chapter 2, paragraph D and G)			
2.1.4.2. Does an appropriate SCI-security official (SSO, SVA Custodian, CSSO, SSR) or their designee, having SCI security cognizance over the unit concerned, conduct the indoctrination? (DoD 5105.21-M-1, chapter 2, paragraph D and G)			
2.1.4.3. Does the unit use tapes or brochures that are tailored to the local SCI environment to supplement the briefing? (DoD 5105.21-M-1, chapter 2, paragraph D and G)			
2.1.4.4. Does the unit require the individual to sign a Nondisclosure Statement (NDS) (if one was not previously signed) prior to SCI indoctrination? (DoD 5105.21-M-1 chapter 2, paragraph G.1)			
2.1.4.5. Does the unit immediately terminate the SCI-indoctrination process if the individual refuses to sign the NDS? (DoD 5105.21-M-1, chapter 2, paragraph G.1.b(3))			
2.1.4.6. Are NDSs completed and the original forwarded to 497 IG/INS? (AFMAN 14-304, paragraph 2.3.3; DoD 5105.21-M-1, chapter 2, paragraph G.1.b(6))			
2.1.4.7. Is the date the NDS was signed tracked by the Security Office? (DoD 5105.21-M-1, chapter 2, paragraph G.1.b(6))			
2.1.4.8. Do SCI-indoctrination memorandums report all accesses authorized? (DoD 5105.21-M-1, chap2, paragraph G.2.b)			
2.1.4.9. Is the original indoctrination memo (DD Form 1847) retained on file? (DoD 5105.21-M-1, chapter 2, paragraph G.2.b)			
2.1.4.10. Does the unit maintain a local roster or register showing the date each person was last indoctrinated? (DoD 5105.21-M-1, chapter 2, paragraph C.1.a)			

2.1.4.11. For units without Sentinel Key: Is an indoctrination message, with names, rank, SSAN, indoctrinate or debrief date, NDS date, accesses, and access number, sent to SSO AIA/SOP? (AFMAN 14-304, paragraph 2.3.2)			
2.1.4.12. Does the unit indoctrination process stress individual responsibilities for reporting changes in personal status to the Security Office? (DoD 5105.21-M-1, chapter 2, paragraph L)			
2.1.4.13. Is a formal screening interview and local records check completed on all requests for SCI or TK special purpose accesses? (AFMAN 14-304, paragraph 2.4.2)			
2.1.4.14. When indoctrinating an individual for special purpose access, is the DD Form 1847 being completed to show this? (AFMAN 14-304, paragraph 2.3.3.1)			
2.1.4.15. Is the original debrief memo (DD Form 1848) retained for 6 months? (DoD 5105.21-M-1, chapter 2, paragraph N.1)			
2.1.4.16. Has the SIO instituted a continuing Security Education Program for all persons having SCI access? (DoD 5105.21-M-1, chapter 2, paragraph P)			
2.1.5. SCI Access Certification:			
2.1.5.1. Do all outgoing "Clearance Visit Notification" messages contain the visitors rank and name; SSAN; clearance level and SCI accesses; dates of visit, purpose of visit; name and telephone number of POC at visit location; contract number if appropriate? (DoD 5105.21-M-1, chapter 6, paragraph C3.a)			
2.1.5.2. Is SSO accepting only SI or TK on contractors from the CSSO? (DoD 5105.21-M-1, chapter 6, paragraph C2.a)			
2.1.5.3. Are outgoing messages marked "Unclassified or For Official Use Only" when using DCI digraphs, trigraphs, and "Top Secret Category III COMINT?" (Certain circumstances, require certification of accesses to be classified) (DoD 5105.21-M-1, chapter 6, paragraph C4)			
2.1.6. Access Management (Billets):			
2.1.6.1. Is a BRAVO Control Officer appointed? (AFMAN 14-304, paragraph 2.1.2)			
2.1.6.2. Are requests for BRAVO accesses forwarded to the MAJCOM, FOA, or DRU? (AFMAN 14-304, paragraph 2.1.2)			
2.1.6.3. Does the MAJCOM, FOA, or DRU approve realignment or redesignations of BRAVO accesses? (AFMAN 14-304, paragraph 2.1.2)			
2.1.6.4. Does the unit send an annual report to HQ AIA/SOP giving the total number of persons briefed for SCI access as of 30 Sep and the number briefed for SI, TK, G, and B compartments? (DoD 5105.21-M-1, chapter 2, paragraph O)			
2.1.7. Access Management (Contractors):			

2.1.7.1. Have copies of the original DD Form 254, DoD Contract Security Classification Specification, been forwarded to the local SSO the same day the billet request is forwarded and has the contract monitor or CSSO endorsed all 254s? (DoD 5105.21-M-1, chapter 2, paragraph E.2; AFMAN 14-304, chapter 1, paragraph 6.b)			
2.1.7.2. Are DD Form 254s current and accurate for all contracts held by the SSO? (DoD 5105.21-M-1, chapter 2, paragraph E.2)			
2.1.7.3. Are contractor files maintained for each company and individual contracts held by the local SSO or unit? (DoD 5105.21-M-1, chapter 1, paragraph F5a(16); AFMAN 14-601, paragraph 1.4)			
2.1.8. Access Management (Transfer-in-Status (TIS)):			
2.1.8.1. Has the unit established a procedure to ensure a TIS request has been submitted on all projected personnel requiring SCI access and having a current SSBI? (DoD 5105.21-M-1, chapter 2, paragraph J; AFMAN 14-304, paragraph 2.6)			
2.1.8.2. Does the TIS departure message contain all the required information; name, rank, SCI access being transferred, anticipated reporting date (TDY organization, if required), POC and phone number? (DoD 5105.21-M-1, chapter 2, Appendix E, Annex 5; AFMAN 14-304, Figure 2.9)			
2.1.8.3. Is HQ AIA/SOP an information addressee on all TIS request and departure messages? (AFMAN 14-304, Figure 2.8 & 2.9)			
2.1.8.4. Are individuals debriefed from additional accesses not requested in TIS request? (DoD 5105.21-M-1, chapter 2, paragraph J.1)			
2.1.8.5. Have military and civilian personnel been debriefed upon separation or retirement before indoctrination as a contractor? (DoD 5105.21-M-1, chapter 2, paragraph J.3)			
2.1.8.6. Does the SSO ensure a DISCO Top Secret has been received before authorizing the contractor TIS action? (AFMAN 14-304, paragraph 2.6.2.1)			
2.2. NONCRITICAL ITEMS:	**YES**	**NO**	**N/A**
2.2.1. Marriage to non-US Citizens:			
2.2.1.1. Are SCI indoctrinated individuals notifying the SSO, in writing, of their intent to marry a non-US citizen? (ODANS 06-97, AFMAN 14-304, paragraph 2.7.2)			
2.2.1.2. Does the intent to marry statement include the following information? (ODANS 06-97, AFMAN 14-304, paragraph 2.7.2)			
2.2.1.2.1. A statement of intent to marry?			
2.2.1.2.2. Name, address, citizenship, and vocation of intended spouse and immediate family members?			
2.2.1.2.3. A comment indicating whether or not family members have political or vocational ties to any government?			
2.2.1.2.4. Nature and extent of contact with immediate family members			
2.2.1.2.5. Whether or not member is cohabiting with the intended spouse?			

2.2.1.2.6. If cohabiting, the date the cohabitant Single Agency Check (SAC) was initiated?			
2.2.1.3. Is "Authority to Proceed" requested from HQ AIA/SOPS prior to allowing the marriage of an SCI indoctrinated person to a non-US citizen? (ODANS 06-97, AFMAN 14-304, paragraph 2.7.2)			
2.2.1.4. Are spouse or cohabitant SACs (DD 1879 on the AF affiliated individual and SF 86, items 1-6 and 8 on the new spouse or cohabitant) submitted to DSS on the new spouse or cohabitant with the results forwarded to the 497 IG/INSA? (ODANS 06-97, AFMAN 14-304, paragraph 2.7.2)			
2.2.1.5. If the spouse SAC uncovers significant derogatory information is a SIF established? (ODANS 06-97, AFMAN 14-304, paragraph 2.7.2)			
2.2.1.6. Is a record kept of the spouse or cohabitant SACs submitted? (ODANS 06-97, AFMAN 14-304, paragraph 2.7.2)			
2.2.2. Special Access Program (SAP)			
2.2.2.1. Are procedures followed when an Air Force Activity has a need to establish a SAP? (DoD 5200.1R, chapter 8)			
2.2.2.2. Does the office of primary responsibility (OPR) of each SAP conduct a review annually showing rationale for it's continuance? (DoD 5200.1-R & E.O. 12958)			
2.2.2.3. Does the OPR conduct and document an annual review of each approved SAP? (E.O. 12958)			
2.2.2.4. Are materials stored only in program-approved storage facilities and security containers? (AFI 16-701, Atch 6)			

Table A2.3. Checklist for Industrial Security.

SECTION 3: INDUSTRIAL SECURITYMISSION STATEMENT: Set forth policies, practices, and procedures to be followed by user agencies for the effective protection of classified information provided to industry, including foreign classified information the US Government is obliged to protect in the interest of national security.**NOTE:** All references are from AFI 31-601, unless otherwise stated.			
3.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
3.1.1. Servicing Security Activity Management:			
3.1.1.1. Does the SSA conduct security reviews according to the National Industrial Security Program Operating Manual (NISPOM)? (paragraph 1.4.1)			
3.1.1.2. Does the SSA review draft security classification guides and DD Form 254, (DoD Contract Security Classification Specifications), for accuracy and completeness? (paragraph 1.4.1)			
3.1.1.3. Are security reviews or self-inspections conducted in accordance with DoD 5200.1 R or AFI 31-401, *Information Security Program*, or installation security program requirements? (paragraph 1.4.1)			

3.1.1.4. Prior to the review, was a check of all appropriate correspondence checked, i.e., DD Form 254, **Statement of Work, Visitor Group Security Agreement (VGSA)**, etc.? (AFH 31-602, paragraph 6.1.5.1.3)			
3.1.1.5. Does the SSA help incorporate appropriate security requirements in classified contracts? (paragraph 1.4.1)		‘	
3.1.1.6. Does the SSA coordinate with other groups within the Air Force to provide specialized expertise when necessary to complete a review (i.e. OPSEC, COMPUSEC, COMSEC, etc.)? (paragraph 1.6.3)			
3.1.1.7. Are draft consultations with the SSA documented in the remarks section (Block 13) of the DD Form 254? (paragraph 4.2.3)			
3.1.1.8. Does the SSO manage, supervise, and provide SCI support to DoD SCI contractors, including the processing, review, and approval of DD Form 254 (Contract Security Classification Specification), and to Special Access Programs? (DoD 5105.21-M-1, chapter 1, paragraph F.5.a(16))			
3.1.1.9. Does the contracting officer’s representative(s) maintain records of accountable SCImaterial provided to the contractor and provide CSSO with a listing of such accountable documents by contract number, document accountability number, copy number, and document title? (DoD 5105.21-M-1, chapter 1 paragraph 3.2.3.)			
3.1.1.10. Has the DD form 254 been completed? (AFH 31-602, chapter 9)			
3.1.1.11. Are visitor groups authorized to operate in accordance with DoD 5200.1-R, clearly identifying what specific security requirements are applicable to the visitor group in the Visitor Group Security Agreement (VGSA)? (AFH 31-602, paragraph 3.2.3.)			
3.2.1. NONCRITICAL ITEMS			
3.2.2.1 Cleared Facility Reviews			
3.1.2.2. Does the SSA provide DSS Cognizant Security Office (CSO) a copy of the security review and survey reports which pertain to on-base cleared facilities? (paragraph 1.6.4.1)			
3.1.2.3. Has the DD Form 696, **Industrial Security Inspection Report**, been completed? (AFH 31-602, paragraph 6.1.1)			
3.1.2.4 How often are security reviews conducted of cleared facilities? (**NOTE:** No more than every 12 months.) (AFH 31-602, paragraph 6.1.2)			
3.1.2.5. Has the cleared facility been given at least 30 days written notice prior to the security review? (AFH 31-602, paragraph 6.1.3)			
3.1.2.6. Does the security review check for compliance in the contractor's security program? (AFH 31-602, paragraph 6.1.4.1)			
3.1.2.7. Does the security review identify weaknesses in the contractor's security program? (AFH 31-602, paragraph 6.1.4.1)			
3.1.2.8. Are corrective actions identified during security reviews? (AFH 31-602, paragraph 6.1.4.1)			

3.1.2.9. Prior to the review, was the previous review record checked? (AFH 31-602, paragraph 6.1.5.1.1)			
3.1.5.8. Prior to the review, were the security violation reports since the previous review checked? (AFH 31-602, paragraph 6.1.5.1.2)			
3.1.5.10. Are meetings scheduled with the contractor's senior on-base management officials prior to the beginning of the formal security review? (AFH 31-602, paragraph 6.1.6.1)			
3.1.5.11. Are unannounced security reviews conducted for cause (i.e., unsatisfactory rating, major deficiency, etc.) to confirm that appropriate corrective actions have been initiated, taken, or implemented which properly protect classified information? (AFH 31-602, paragraph 6.1.8.1)			
3.1.5.12. Are exit briefings conducted with the on-base contractor's senior management officials at the conclusion of the security review? (AFH 31-602, paragraph 6.1.9.1)			
3.1.5.13. Has only generic references been made to minor administrative issues? (AFH 31-602, paragraph 6.1.9.2)			
3.1.5.14. Are the positive aspects of the contractor's security program stressed during exit briefings? (AFH 31-602, paragraph 6.1.9.2)			
3.1.5.15. Are unsatisfactory ratings given when the results of the security review demonstrates the contractor's inability or unwillingness to properly safeguard classified information? (AFH 31-602, paragraph 6.1.10.1)			
3.1.5.16. Are unsatisfactory ratings given when the results of the security review demonstrates the contractor's repeated failure to correct major deficiencies? (AFH 31-602, paragraph 6.1.10.1)			
3.1.5.17. Are security reviews rated "unsatisfactory" promptly reported to the contracting office and the Cognizant Security Office (CSO)? (AFH 31-602, paragraph 6.1.10.2)			
3.1.5.18. Does the SSA make recommendations to the CSO via the contracting office, concerning facility clearance (FCL) revocation? (AFH 31-602, paragraph 6.1.10.3)			
3.1.6. Visitor Group Security Reviews:			
3.1.6.1. Are security reviews conducted for visitor groups operating under DoD 5200.lR or AFI 31-401, *Information Security Program*? (AFH 31-602, paragraph 6.2.1)			
3.2. NONCRITICAL ITEMS:	**YES**	**NO**	**N/A**
3.2.1. Does the Servicing Security Activity (SSA) maintain contract folders on each cleared facility and visitor group that has access to classified information? (paragraph 1.4.1)			
3.2.2. Does the SSA help incorporate appropriate security requirements in classified contracts? (paragraph 1.4.1)			
3.2.3. Are draft consultations with the SSA documented in the remarks section (Block 13) of the DD Form 254? (paragraph 4.2.3)			

3.2.4. Has a contract monitor been appointed to administer each SCI contract? (DoD 5105.21-M-1, chapter 1, paragraph F(4)a)			
3.2.5. Does the contract monitor verify that all SCI material released to a contractor is essential to contract accomplishment? (DoD 5105.21-M-1, chapter 1, paragraph F(6)e)			
3.2.6. Does the unit obtain the originator's permission prior to releasing SCI material to a contractor or consultant? (DoD 5105.21-M-1, chapter 1, paragraph F(6)e)			
3.2.7. Does the contract monitor maintain records of all SCI material products released to contractors or consultants? (DoD 5105.21-M-1, chapter 1, paragraph F(6)f)			
3.2.8. Does the SSO manage, supervise, and provide SCI support to DoD SCI contractors, including the processing, review, and approval of DD Form 254 (Contract Security Classification Specification), and to Special Access Programs? (DoD 5105.21-M-1, chapter 1, paragraph F. 5.a (16))			
3.2.9. Does the contracting officer's representative(s) (COR) prepare or review contract justification for SCI access; ensures completeness of the information? (DoD 5105.21-M-1, chapter 1, paragraph F.6.c)			

Table A2.4. Physical Security.

SECTION 4: PHYSICAL SECURITYMISSION STATEMENT: To ensure all Air Intelligence Agency (AIA) and AIA supported units meet construction and security standards for US-government sponsored and contractor facilities where sensitive compartmented information (SCI) may be stored, used, discussed and, or processed.**NOTE:** All references are from DCID 1/21 unless otherwise stated.			
4.1. CRITICAL ITEMS.	**YES**	**NO**	**N/A**
4.1.1. Sensitive Compartmented Information Facility (SCIF) Management:			
4.1.1.1. Are perimeter walls, floors, and ceilings constructed according to the approved Fixed Facility Checklist (FFC)? (Annex A)			
4.1.1.2. When vault doors are left open, is a separate door used to control daytime access? (paragraph 3.3.3.4)			
4.1.1.3. Are door hinges protected against unauthorized removal? (paragraph 3.3.3.3(a))			
4.1.1.4. Are exposed door locks, left open in an uncontrolled area, protected against unauthorized access or tampering? (paragraph 3.3.3.3(b))			
4.1.1.5. Are vents and ducts, and similar openings in excess of 96 sq. inches that enter or pass through the SCIF, properly alarmed (OUTSIDE CONUS) and protected with sound baffles and are access ports locked if installed outside the SCIF perimeter? (paragraph 3.3.4.1)			

4.1.1.6. Are all windows, which might afford visual surveillance of the interior of the SCIF, made opaque or equipped with blinds or other such coverings, and all windows at ground level (less than 18 feet above the ground) covered by an IDS? (paragraph 3.3.5)			
4.1.1.7. If a separate intercom, paging and, or public address system is installed, separate of the approved phone system, is it installed or certified as applicable? (AFSSM 7011, paragraph 8.53; NSTISSAM 2-95, paragraph 4.9.2)			
4.1.1.8. Are physical security requirements for tactical SCIFs established? (Annex C)			
4.1.1.9. Are all intrusion detection systems (IDS) accepted by the Cognizant Security Authority (CSA) and, or UL listed (or equivalent as defined by the CSA) and reflected in the current accreditation package? (Annex B, paragraph 3.2)			
4.1.1.10. SCIFs OUTSIDE US: Are doors, walls, and areas above false ceilings protected as required by CSA? (Annex B, paragraph 3.6)			
4.1.1.11. Is emergency power provided to the SCIF IDS and does the emergency power comply with UL603 ? (Annex B, paragraph 3.5.7.1)			
4.1.1.12. Is there Class I or II transmission line security when IDS transmission lines leave the SCIF and traverses an uncontrolled area ? (Annex B, paragraph 3.5.1)			
4.1.1.13. Does each SCIF have an accreditation file and does the file contain current copies of the FFC; accreditation authorization documents (e.g., physical, TEMPEST, & AIS); inspection reports, including TSCM reports; operating procedures; Special Security Officer (SSO) or Contractor Special Security Officer (CSSO) appointment letters; Memorandum Of Agreement (MOA); Emergency Action Plan (EAP); etc? (paragraph 2.3.3; AFMAN 14-304, paragraph 5.8)			
4.1.1.14. Does the locally designated SCI security official notify the CSA, MAJCOM SSO, and the supporting SSO of changes that significantly affect the SCIF's security posture? (AFMAN 14-304, paragraph 5.10)			
4.1.1.15. Is a pre-construction approval package submitted for new SCIFs and for proposed significant modifications to existing SCIFs? (AFMAN 14-304, paragraph 5.7.3.2)			
4.1.1.16. Is the alarm system tested semi-annually and is a record of IDE testing being maintained at the SCIF that reflects testing date, individuals who performed the test, specific equipment tested, malfunctions, and corrective actions taken? (Annex B, paragraph 3.8.1)			
4.1.1.17. Are tests of the response force being conducted semi-annually and is a record of response force testing being maintained ? (Annex B, paragraph 3.8.1)			
4.2. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
4.2.1. Entry Credentials:			

4.2.1.1. Are AIA entry credentials requisitioned through the local Publication Distribution Office? (AFI 31-101, paragraph 9.4.1)			
4.2.1.2. Are AIA entry credentials physically inventoried by serial number and the sender notified of any discrepancies? (AFI 31-101, paragraph 9.5.1)			
4.2.1.3. Is each series of forms (AIA Forms 325, 325T, etc.) entered on a separate AF Form 335, Issuance Record-Accountability Identification Card, upon receipt from the distribution office? (AFI 31-101, paragraph 9.5.1.1)			
4.2.1.4. Are AIA temporary badges distinctively marked; are personnel utilizing temporary badges positively identified at the Entry Control Point (ECP); does the temporary badge remain within the restricted area? (AFI 31-101, paragraph 9.6.2)			
4.2.1.5. Is a copy of AF Form 213, Receipt for Accountability Form, filed with reports of investigation for lost badges and certification of destruction? (AFI 31-101, paragraph 9.5.1.2)			
4.2.1.6. Are blank entry credentials stored, as a minimum, in a locked steel cabinet? (AFI 31-101, paragraph 9.4.2)			
4.2.1.7. Does the installation CSF conduct a thorough investigation into missing blank AIA entry credential forms? (AFI 31-101, paragraph 9.4.6.1)			
4.2.1.8. When a person loses their AIA entry credential, does the appropriate security manager investigate the facts surrounding the loss? (AFI 31-101, AIA Sup 1, paragraph 9.4.6)			
4.2.1.9. Is a physical audit and inventory of AIA entry credentials conducted annually? (AFI 31-101, paragraph 9.5.2)			
4.2.1.10. Is an audit conducted when the AIA entry credential issuing official changes? (AFI 31-101, paragraph. 9.5.2)			
4.2.1.11. Are surrendered or confiscated badges destroyed immediately unless they are being held pending the outcome of final decision to disqualify personnel? (AFI 31-101, paragraph 9.2.7)			
4.2.1.12. Is the destruction of surrendered or confiscated badges recorded? (AFI 31-101, paragraph 9.5.3.3)			
4.1.2.13. Are procedures in effect to collect an individual's AIA entry credential when entry authority has been withdrawn? (AFI 31-101, paragraph 5.3.9.4; AIA Sup 1, paragraph 9.5.3.1)			
4.2.1.14. Is the unit using AIA Form 31, **Entry Authority/Badge Issue/Security Training Card**, or computer-generated products, instead of AF Form 2586, **Unescorted Entry Authorization Certificate**, to request and issue AIA entry credentials? (AFI 31-101, AIA Sup 1, paragraph 5.2)			
4.3. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
4.3.1. Emergency Action Plans (EAP) or Emergency Destruction Plans (EDP):			
4.3.1.1. Has an EAP been established? (DoD 5105.21-M-1, chapter 5, section H)			

4.3.1.2. Has the EAP been approved by the Senior Intelligence Officer (SIO)? (DoD5105.21-M-1, chapter 5, section H)			
4.3.1.3. Does the EAP take into account natural disaster, labor strife, IDS or alarm outage, and entrance of emergency personnel (e.g. police, medical, and firefighters) into the SCIF? (DoD 5105.21-M-1, chapter 5, section H, paragraph 1)			
4.3.1.4. Does the EAP address adequacy of protection and firefighting equipment, evacuation plans for persons and SCI material, and life-support equipment (e.g. oxygen and masks)? (DoD 5105.21-M-1, chapter 5, section H, paragraph 1)			
4.3.1.5. If the SCIF is located in an area of political instability, terrorism, host country attitude, or where criminal activity suggests the possibility that a SCIF might be overrun by hostile forces, does the EAP provide for the secure destruction or removal of SCI material under adverse conditions? (DoD 5105.21-M-1, chapter 5, section H, paragraph 2)			
4.3.1.6. If the risk of overrun is significant, is the amount of SCI holdings reduced to, and kept at, the minimum needed for current working purposes? (DoD 5105.21 -M-1, chapter 5, section H, paragraph 2)			
4.3.1.7. Are all personnel familiar with the EAP? (DoD 5105.21 -M-1, chapter 5, section H, paragraph 3)			
4.3.1.8. Has the EAP been reviewed annually and updated as necessary? (DoD 5105.21-M-1, chapter 5, section H, paragraph 3 and Appendix G, paragraph 1(d); AFMAN 14-304, paragraph 5.13)			
4.3.1.9. In areas where political or criminal activity suggests the possibility that a SCIF might be overrun, does the SSO or CSSO conduct drills to ensure testing and adequacy of the EAP? Are drills conducted as circumstances warrant and no less frequently than annually? (DoD 5105.21-M-1, chapter 5, section H, paragraph 3)			
4.3.1.10. Has SCI material identified for emergency destruction or removal been labeled as: (DoD 5105.21-M-1, chapter 5, section H, paragraph 4)			
4.3.1.10.1. Priority One: All cryptographic equipment and documents			
4.3.1.10.2. Priority Two: All operational SCI codeword material which might divulge targets and successes, documents dealing with U.S. SCI activities, and documents concerning compartmented projects and other sensitive intelligence materials and Top Secret collateral			
4.3.1.10.3. Priority Three: Less sensitive administrative SCI material and collateral classified material not included above			
4.3.1.11. Does the EAP address the following items: (DoD 5105.21-M-1, Appendix G, paragraph 2 (a-n))			
4.3.1.11.1. Location of fire fighting equipment.			
4.3.1.11.2. Assignment of specific responsibilities by duty position, with alternates.			

4.3.1.11.3. Authorization for the senior individual present to implement the plan.			
4.3.1.11.4. Periodic review of assigned duties by all personnel.			
4.3.1.11.5. Location of SCI material by storage container.			
4.3.1.11.6. Location of safe combinations.			
4.3.1.11.7. Procedures for admitting uncleared emergency personnel into the SCIF and provisions for safeguarding SCI material during such access.			
4.3.1.11.8. Removal of SCI document accounting records to facilitate the post-emergency inventory.			
4.3.1.11.9. Emergency evacuation procedures for equipment, material, and personnel, as appropriate.			
4.3.1.11.10. Emergency storage procedures, if appropriate.			
4.3.1.11.11. Provisions for precautionary and complete destruction, if appropriate.			
4.3.1.11.12. Designation of evacuation site and alternate site.			
4.3.1.11.13. Designation of primary and alternate travel routes.			
4.3.1.11.14. Provisions for packing, loading, transporting, and safeguarding SCI material.			
4.3.1.12. For SCIFs located outside the US does the EAP address the following additional items: (DoD 5105.21-M-1, Appendix G, paragraph 3 (a-d))			
4.3.1.12.1. Location of destruction equipment?			
4.3.1.12.2. Periodic checks of all incendiary devices?			
4.3.1.12.3. Minimum retention of SCI material?			
4.3.1.12.4. Close coordination with, or incorporation into, host command's emergency contingencies?			
4.3.1.13. For SCIFs located in the US, has evacuation or storage been considered before destruction? (DoD 5105.21-M-1, Appendix G, paragraph 5)			
4.3.1.14. Are the time limits attainable? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8a(2))			
4.3.1.15. Are policies and procedures established to keep the volume of classified holdings at the lowest level consistent with operational necessity? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8b(l))			
4.3.1.16. Are computer databases, compact discs, and microfilms used to the maximum extent possible? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8b(l))			
4.3.1.17. Are procedures established for periodic inventories of sensitive material held at field stations, and destruction equipment and media? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8b(2))			
4.3.1.18. Is a review of sensitive material conducted by the Chief of Field Stations by 15 January of each year and the results reported? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8c(l))			

4.3.1.19. Has the EDP been coordinated with the host agency and is it in writing? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8c(2))			
4.3.1.20. Are all persons assigned duties in the EDP familiar with their duties? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8c(3))			
4.3.1.21. Are rehearsals conducted quarterly, exclusive of any other EAP exercises? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8c(4))			
4.3.1.22. Is an emergency destruction officer identified? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8c(6))			
4.3.1.23. Is emergency power (controlled by US personnel) available? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8e(3))			
4.3.1.24. Is destruction equipment shielded from exposure and readily available? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8e(4))			
4.3.1.25. Are means of transporting material to the destruction site available? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8e(4))			
4.3.1.26. Are all safes, equipment, or other containers of classified material marked to indicate the appropriate destruction priority? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8e(5))			
4.3.1.27. Does the EDP include the use of individual cards, listing specific tasks to be performed by assigned personnel in execution of the EDP? ((U) USSID 3 (C/SI), Annex B, paragraph 2.8g(5))			
4.4. NONCRITICAL ITEMS:	**YES**	**NO**	**N/A**
4.4.1. Temporary Secure Working Areas (TSWA):			
4.4.2. Has approval to process SCI in a TSWA been received from the CSA? NOTE: HQ AIA/SOX is the approval authority for discussion/handling of SCI (paragraph 3.2.2)			
4.4.3. Is the TSWA secured with an alarm? (NOTE: Recommended, but not required) (paragraph 3.2.2)			
4.4.4. Is the TSWA used more than 40 hours per month? If yes, was permission granted by the CSA for no longer than 6 months? (paragraph 3.2.1)			
4.4.5. Is SCI material stored in the TSWA? If yes, was permission granted by the CSA for no longer than six months? (paragraph 3.2.1)			
4.4.6. During use, is entrance to the TSWA controlled and only authorized personnel permitted entry? (paragraph 3.2.2)			
4.4.7. Does the TSWA meet sound attenuation guidelines? (paragraph 3.2.2 and Annex E)			
4.4.8. If required by the CSA, was a Technical Surveillance Countermeasures (TSCM) sweep conducted? (paragraph 3.2.2)			
4.4.9. When not in use, is the TSWA secured with a key or combination lock approved by the CSA? (paragraph 3.2.3(a))			
4.4.10. When not in use, is access to the TSWA limited to personnel with a US Secret clearance? (paragraph 3.2.3(b))			

4.5. NONCRITICAL ITEMS:	YES	NO	N/A
4.5.1. Tactical SCIFs (T-SCIF) (Ground Operations):			
4.5.1.1. Have efforts been made to obtain the necessary support from the host command? (Annex C, Part 1, paragraph 2.0)			
4.5.1.2. If under field or combat conditions, is 24-hour operations conducted? (Mandatory) (Annex C, Part 1, paragraph 2.0)			
4.5.1.3. Are minimum physical security requirements and security considerations for permanent secure facilities being continuously pursued if the situation and time permits? (Annex C, Part 1, paragraph 2.0)			
4.5.1.4. Is the T-SCIF located within the supported headquarters defensive perimeter? And preferably within the Tactical Operations Center (TOC) perimeter? (Annex C, Part 1, paragraph 2.1)			
4.5.1.5. Is the T-SCIF established and clearly marked using a physical barrier? (Annex C, Part 1, paragraph 2.2)			
4.5.1.6. If practical, is the T-SCIF barrier composed of triple strand concertina or general purpose barbed tape obstacle (GPBTO)? (Annex C, Part 1, paragraph 2.2)			
4.5.1.7. Has the T-SCIF approving authority approved the security measures based upon the local threat conditions? (Annex C, Part 1, paragraph 2.2)			
4.5.1.8. Is the perimeter guarded by walking or fixed guards? (Annex C, Part 1, paragraph 2.3)			
4.5.1.9. Are the guards providing observation of the entire controlled area? (Annex C, Part 1, paragraph 2.3)			
4.5.1.10. Are the guards equipped with weapons and ammunition? (Annex C, Part 1, paragraph 2.3)			
4.5.1.11. Are the weapons the type prescribed by the supported commander? (Annex C, Part 1, paragraph 2.3)			
4.5.1.12. Is the access to the controlled area restricted to a single entrance or gate, which is guarded on a continuous basis? (Annex C, Part 1, paragraph 2.4)			
4.5.1.13. Is an access list maintained? (Annex C, Part 1, paragraph 2.5)			
4.5.1.14. Is access restricted to those personnel whose names appear on the access lists? (Annex C, Part 1, paragraph 2.5)			
4.5.1.15. Is the T-SCIF staffed with sufficient personnel as deemed by the on-site security authority? Is this decision based upon the local threat conditions? (Annex C, Part 1, paragraph 2.6)			
4.5.1.16. Are emergency destruction and evacuation plans kept current? (Annex C, Part 1, paragraph 2.7)			
4.5.1.17. When not in use, is SCI material stored in lockable or approved containers? (Annex C, Part 1, paragraph 2.8)			
4.5.1.18. If possible, has communications been established with backup response forces? (Annex C, Part 1, paragraph 2.9)			

4.5.1.19. Has the SSO or designee, conducted an inspection of the vacated T-SCIF area to ensure SCI materials were not left behind? (Annex C, Part 1, paragraph 2.10)			
4.5.1.20. If required by approving authorities, has a local tactical security deployment checklist been submitted? (Annex C, Part 1, paragraph 4.1)			
4.5.1.21. If initiated during a period of declared hostilities or general war, has a general or flag officer established the level of accreditation? (Annex C, Part 1, paragraph 3.0)			
4.5.1.22. If used to support a field training exercise, has the SIO taken responsibility? (Annex C, Part 1, paragraph 3.0)			
4.5.1.23. Has a message requesting the establishment of a T-SCIF been sent to the CSA or designee, prior to commencement of SCIF operations? (Annex C, Part 1, paragraph 4.2)			
4.5.1.24. Was the first consideration of the establishment of a T-SCIF the effective and secure accomplishment of the mission? (Annex C, Part 1, paragraph 5.0)			
4.5.1.25. If the T-SCIF is a rigid side shelter or portable van, has it been equipped with a combination lock that meets federal specifications of FF-L-2740 or other CSA approved locks? (Annex C, Part 1, paragraph 6.1)			
4.5.1.26. Is the combination to the lock stored and controlled at the same level of security for which the T-SCIF is accredited? (Annex C, Part 1, paragraph 6.1)			
4.5.1.27. Is the shelter or van secured at all times when not activated as a T-SCIF? (Annex C, Part 1, paragraph 6.1)			
4.6. NONCRITICAL ITEMS:	**YES**	**NO**	**N/A**
4.6.1. Tactical SCIFs (T-SCIF) (Airborne Operations)			
4.6.1.1. If initiated during hostilities or general war, has a general or flag officer established the level of accreditation? (Annex C, Part 11, paragraph 3.0)			
4.6.1.2. Has a message or letter requesting the establishment of an aircraft or airborne SCIF been sent to the approving authority prior to the commencement of SCIF operations? (Annex C, Part 11, paragraph 4.2)			
4.6.1.3. If required by approving authorities, has a local deployment checklist been submitted? (Annex C, Part 11, paragraph 4.1)			
4.6.1.4. If used to support a field training exercise, has the SIO taken responsibility? (Annex C, Part 11, paragraph 3.0)			
4.6.1.5. Is the SCIF staffed with sufficient personnel as deemed by the on-site security authority? Is this decision based upon the local threat environment? (Annex C, Part 11, paragraph 4.3)			
4.6.1.6. If feasible, has SCI material been removed from the aircraft upon completion of the mission or at any landings? (Annex C, Part 11, paragraph 4.4)			

4.6.1.7. If removal is not possible, or when suitable storage space or locations are not available, have two armed (with ammunition) SCI-indoctrinated personnel remain with the aircraft ? (Annex C, Part 11, paragraph 4.4)			
4.6.1.8. If personnel do not have weapons and ammunition, has a waiver been approved by the commander? (Annex C, Part 11, paragraph 4.4)			
4.6.1.9. Has the SSO, or senior SCI-cleared person, conducted an inspection of the vacated SCIF to ensure SCI materials were not left behind? (Annex C, Part 11, paragraph 4.5)			
4.6.1.10. If not protected by an approved IDS, are hourly inspections made of all hatches and seals, including seal numbers, of accredited aircraft? (Annex C, Part 11, paragraph 5.1)			
4.6.1.11. Is a guard force and response team available for accredited aircraft, and are they capable of responding within 5 minutes for open storage and 15 minutes for closed storage? (Annex C, Part 11, paragraph 5.2)			
4.6.1.12. For aircraft that are parked outside an established controlled area, has a temporary controlled area been established? (Annex C, Part 11, paragraph 5.3)			
4.6.1.13. If no SCI-cleared individuals are with the aircraft, has the commander or crew members left the aircraft guarded by a guard force member who has been subjected to at least a trustworthiness determination? (Annex C, Part 11, paragraph 6.1)			
4.6.1.14. Are all hatches locked and, or sealed to prevent unauthorized entry? (Annex C, Part 11, paragraph 6.2)			
4.6.1.15. For unscheduled aircraft landings:			
4.6.1.15.1. On US military bases, has the local SSO or base security officer been notified of the estimated arrival times and security protection required? (Annex C, Part 11, paragraph 8.1)			
4.6.1.15.2. On other airfields within the US, has the local Federal Aviation Administration (FAA) security officer been notified of the estimated arrival time and security protection required? (Annex C, Part 11, paragraph 8.2.1)			
4.6.1.15.2.1. Upon arrival, was the senior SCI-indoctrinated person responsible for controlling entry and maintaining surveillance over the aircraft until SCI material could be secured in an accredited SCIF or the aircraft departs? (Annex C, Part 11, paragraph 8.2.2)			
4.6.1.15.2.2. If a properly accredited US Government SCIF can't be used for temporary storage was the SCI material double wrapped with initialed seals and stored in a GSA approved security container? (Annex C, Part 11, paragraph 8.2.3)			
4.6.1.15.3. In unfriendly territory, was all SCI material immediately destroyed, with the destruction preferably taking place prior to landing? (Annex C, Part 11, paragraph 8.3)			

4.6.1.15.3.1. Was the mission carefully planned so that SCI material was kept to the absolute minimum for mission accomplishment? (Annex C, Part 11, paragraph 8.3.1)			
4.6.1.15.3.2. Do all personnel rehearse emergency destruction procedures before each mission? (Annex C, Part 11, paragraph 8.3.2)			
4.6.1.15.3.3. Are the emergency destruction rehearsals made a matter of record? (Annex C, Part 11, paragraph 8.3.2)			
4.6.1.16. Are all SCI discussions conducted via appropriately encrypted aircraft radio? (Annex C, Part 11, paragraph 9.0)			
4.6.1.17. Is the EAP written to provide for the evacuation and, or destruction of classified material? (Annex C, Part 11, paragraph 10.1)			
4.6.1.18. Is the EAP approved by the CSA? (Annex C, Part 11, paragraph 10.1)			
4.6.1.19. Is the EAP tested by mission personnel? (Annex C, Part 11, paragraph 10.1)			
4.6.1.20. Is the EAP current? (Annex C, Part 11, paragraph 10.2)			
4.7. NONCRITICAL ITEM:	**YES**	**NO**	**N/A**
4.7.1. Mobile SIGINT SCIFs			
4.7.1.1. Is the T-SCIF under 24 hour continuous operation? (Mandatory) (Annex C, Part 1, paragraph 8.1)			
4.7.1.2. Is the T-SCIF staffed with adequate personnel as determined by the on-site security authority? (Annex C, Part 1, paragraph 8.2)			
4.7.1.3. Have external security measures been incorporated into the perimeter defense plans for the immediate area where the T-SCIF is located? (NOTE: A physical barrier is not required as a prerequisite to establish a mobile SIGINT T-SCIF.) (Annex C, Part 1, paragraph 8.3)			
4.7.1.4. When possible, have communications been established and maintained with backup guard forces? (Annex C, Part 1, paragraph 8.4)			
4.7.1.5. Does the EAP incorporate the use of incendiary devices to ensure total destruction of SCI material in emergency situations? (Annex C, Part 1, paragraph 8.5)			
4.7.1.6. If a rigid-side shelter is used, is it mounted to the vehicle in such a way as to provide the shelter with the capability of moving on short notice? (Annex C, Part 1, paragraph 8.6.1.1)			
4.7.1.7. Has a GSA approved container been permanently affixed within the shelter? (Annex C, Part 1, paragraph 8.6.1.2)			
4.7.1.8. Is the combination to the security container protected to the same level of the material stored within? (Annex C, Part 1, paragraph 8.6.1.2)			
4.7.1.9. Is entrance to the T-SCIF controlled by SCI indoctrinated personnel on-duty within the shelter? (Annex C, Part 1, paragraph 8.6.1.3)			

4.7.1.10. If no one is on-duty in the shelter, is all classified stored within the locked GSA approved container and is the exterior door to the shelter secured? (Annex C, Part 1, paragraph 8.6.1.3)			
4.7.1.11. Is entrance to the T-SCIF limited to only SCI indoctrinated personnel with an established need-to-know? (Annex C, Part 1, paragraph 8.6.1.4)			
4.7.1.12. If the use of a rigid-side container or portable van is not feasible, is the material secured in a container that prevents unauthorized viewing? (Annex C, Part 1, paragraph 8.6.2.1)			
4.7.1.13. Is the security container kept under constant possession of an SCI indoctrinated person? (Annex C, Part 1, paragraph 8.6.2.2)			
4.7.1.14. Is the quantity of SCI material allowed in the T-SCIF limited to that which is absolutely essential to sustain the mission? (Annex C, Part 1, paragraph 8.7)			
4.7.1.15. Are stringent security arrangements employed to ensure large quantities of SCI material are not allowed to accumulate more than is absolutely necessary? (Annex C, Part 1, paragraph 8.7)			
4.7.1.16. Are all working papers generated within the T-SCIF destroyed at the earliest possible time after having served their mission purpose? (Annex C, Part 1, paragraph 8.7.1)			
4.7.1.17. Is a rapid and certain means of destruction available for AIS equipment should the need for total destruction arise? (Annex C, Part 1, paragraph 8.7.2)			
4.8. NONCRITICAL ITEMS:	**YES**	**NO**	**N/A**
4.8.1. Semi-Permanent SCIFs (SPSCIFs)			
4.8.1.1. Is the SPSCIF accredited and operated in the same manner as a permanent SCIF? (Annex C, Part 1, paragraph 9.2)			
4.8.1.2. Is the SPSCIF constructed of such material and composition to show visible evidence of forced entry? (Annex C, Part 1, paragraph 9.3)			
4.8.1.3. Are vents and ducts constructed to prevent surreptitious entry? (Annex C, Part 1, paragraph 9.3)			
4.8.1.4. Are the doors of solid construction and plumbed so the door forms a good acoustical seal? (Annex C, Part 1, paragraph 9.3)			
4.8.1.5. If installed, are emergency exits and escape hatches constructed so they can only be opened from the interior of the SPSCIF? (Annex C, Part 1, paragraph 9.3)			
4.8.1.6. Is the SPSCIF, as determined by the CSA, placed within a fenced compound on a military installation or equivalent? (Annex C, Part 1, paragraph 9.4)			
4.8.1.7. Is the fence placed at least ten feet from the SPSCIF and related buildings and equipment? (NOTE: This distance may need to be greater to provide acoustical security or to meet COMSEC or TEMPEST or EMSEC requirements.) (Annex C, Part 1, paragraph 9.4)			

4.8.1.8. Is the SPSCIF equipped with a combination lock that meets Federal Specification FF-L-2740? (Annex C, Part 1, paragraph 9.5)			